PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :		(11) Internationale Veröffentlichungsnummer:
G07F 7/10	A1	WO 99/57689
		(43) Internationales Veröffentlichungsdatum: 11. November 1999 (11.11.99)

(21) Internationales Aktenzeichen: PCT/EP99/02848

(22) Internationales Anmeldedatum: 27. April 1999 (27.04.99)

(30) Prioritätsdaten:
198 20 422.1 7. Mai 1998 (07.05.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: GIESECKE & DEVRIENT GMBH [DE/DE]; Prinzregentenstrasse 159, D–81677 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: VEDDER, Klaus [DE/DE]; Ainmillerstrasse 38, D–80801 München (DE).

(74) Anwalt: KLUNKER, SCHMITT–NILSON, HIRSCH; Winzererstrasse 106, D–80797 München (DE).

(81) Bestimmungsstaaten: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

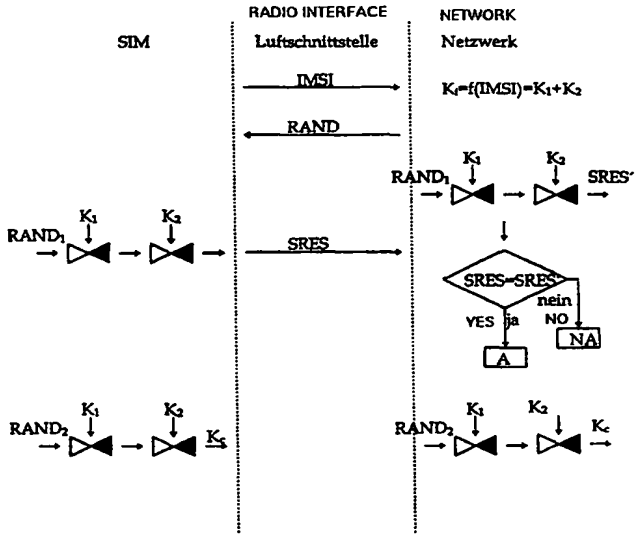
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD FOR AUTHENTICATING A CHIP CARD IN A MESSAGE TRANSMISSION NETWORK

(54) Bezeichnung: VERFAHREN ZUR AUTHENTISIERUNG EINER CHIPKARTE INNERHALB EINES NACHRICHTENÜBERTRAGUNGS–NETZWERKS

(57) Abstract

The invention relates to a method for authenticating a chip card (SIM) in a network for transmitting messages, preferably in a GSM network. According to said method, an optionally secret algorithm and a secret key are stored in a chip card (SIM). In order to authenticate the card, the network or a network component first transmits a random number to the chip card. A reply signal is then generated in said chip card using the algorithm, the random number and the secret key, and transmitted to the network or network component where the authenticity of the card is checked. The authentication message is formed by dividing the secret key and the random number transmitted by the network into at least two parts each. A part of the transmitted random number and one or more parts of the secret key are encoded with a single or multi–stage, preferably symmetrical computation algorithm. A selected part of the product of the encoding procedure is transmitted to the network in order to issue an authentication reply.



(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren zur Authentisierung einer Chipkarte (SIM) in einem Netzwerk zur Nachrichtenübertragung, vorzugsweise in einem GSM–Netzwerk, bei dem in einer Chipkarte (SIM) ein gegebenenfalls geheimer Algorithmus sowie ein geheimer Schlüssel gespeichert ist, wobei zur Authentisierung zunächst vom Netzwerk oder einer Netzwerkkomponente eine Zufallszahl an die Chipkarten übertragen wird, in der Chipkarte mittels des Algorithmus, der Zufallszahl und des geheimen Schlüssels ein Antwortsignal erzeugt wird, das an das Netzwerk bzw. die Netzwerkkomponente übermittelt wird, um dort die Authentizität der Karte zu überprüfen. Gemäß der Erfindung wird zur Bildung der Authentisierungsnachricht sowohl der geheime Schlüssel als auch die vom Netzwerk übertragene Zufallszahl in jeweils wenigstens zwei Teile aufgeteilt, wobei ein Teil der übertragenen Zufallszahl und ein oder mehrere Teile des geheimen Schlüssels mittels eines ein– oder mehrstufigen, vorzugsweise symmetrischen Berechnungsalgorithmus verschlüsselt werden. Zur Ausgabe einer Authentisierungsantwort wird ein auswählbarer Teil des Verschlüsselungsergebnisses an das Netzwerk übertragen.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Verfahren zur Authentisierung einer Chipkarte innerhalb eines Nachrichtenübertragungs-Netzwerks

Die Erfindung betrifft ein Verfahren zur Authentisierung einer Chipkarte in einem Netzwerk zur Nachrichtenübertragung, vorzugsweise in einem GSM-Netzwerk, nach dem Oberbegriff des Anspruchs 1.

Bei GSM-Systemen ist es bekannt, daß sich zum Gebrauch der Chipkarte (Subscriber Identity Module, SIM) zunächst der Benutzer üblicherweise mittels einer persönlichen Identifikationsnummer (PIN) als zur Benutzung berechtigt ausweisen muß. Um an dieser Stelle Mißbrauch zu vermeiden, ist es für die PIN-Eingabe bekannt, einen Fehlerzähler vorzusehen, der nach Überschreiten einer zulässigen Anzahl von Fehlversuchen den weiteren Gebrauch der Karte unterbindet.

Eine weitere systemrelevante Sicherheitsmaßnahme besteht in der Authentisierung der Karte gegenüber dem Mobilfunknetz. Dazu sind in der Karte ein von außen nicht zugänglicher geheimer Schlüssel sowie ein ebenfalls von außen nicht zugänglicher Algorithmus abgelegt. Für eine Authentisierung wird vom Netzwerk bzw. einer Netzwerkkomponente eine Zufallszahl erzeugt und der Karte mitgeteilt. Aus der Zufallszahl und dem geheimen Schlüssel berechnet sodann die Karte mittels des in der Karte vorhandenen Algorithmus eine Antwort, welche sie dem Netzwerk mitteilt. Diese Antwort wird im Netzwerk analysiert und es wird, bei positivem Ergebnis, Zugang zu den Netzwerkfunktionen erlaubt. Die entsprechende Vorgehensweise ist in den einschlägigen GSM-Spezifikationen beschrieben.

Für ein wie vorstehend gesichertes Netz besteht die Gefahr, daß durch Angriffe auf den zur Authentisierung verwendeten Algorithmus das Netzwerk

beispielsweise in einem Computer simuliert werden kann, indem z. B. ausgewählte „Zufallszahlen" nach dem standardisierten Protokoll an die SIM-Karte übermittelt werden und daraus, nach mehrfachen Authentisierungsversuchen, der Geheimschlüssel der Chipkarte ermittelt wird. Ist zusätzlich der Algorithmus der Karte bekannt, können nach Ermittlung des geheimen Schlüssels wesentliche Funktionselemente der Karte simuliert bzw. dupliziert werden.

Es ist deshalb Aufgabe der Erfindung, ein sicheres Verfahren zur Authentisierung einer Chipkarte in einem Nachrichtensystem anzugeben, bei dem, wie beispielsweise im GSM-Netz üblich, eine Rückmeldung über das Authentisierungsergebnis an die teilnehmende Chipkarte nicht erfolgt.

Diese Aufgabe wird gemäß der Erfindung ausgehend von den Merkmalen des Oberbegriffs des Anspruchs 1 durch die kennzeichnenden Merkmale des Anspruchs 1 gelöst.

Vorteilhafte Ausgestaltungen der Erfindung sind in den abhängigen Ansprüchen angegeben.

Die Erfindung sieht vor, zur Bildung der Authentisierungsnachricht sowohl aus dem geheimen Schlüssel als auch aus der vom Netzwerk übertragenen Zufallszahl jeweils wenigstens zwei Teile zu bilden, wobei einer der Teile der übertragenen Zufallszahl und einer oder mehrere Teile des geheimen Schlüssels mittels eines ein- oder mehrstufigen, vorzugsweise symmetrischen Berechnungsalgorithmus verschlüsselt werden. Zur Ausgabe einer Authentisierungsnachricht wird ein auswählbarer Teil des nach dem Authentisierungsalgorithmus berechneten Ergebnisses an das Netzwerk übertragen.

Eine vorteilhafte Ausgestaltung der Erfindung sieht vor, daß in der gleichen Art und Weise auch der Kanalkodierungsschlüssel erzeugt wird, d.h. auch dort ist, beispielsweise bei einer Zweiteilung des Schlüssels und der Zufallszahl vorgesehen, daß entweder der erste oder der zweite Teil der übertragenen Zufallszahl mit dem ersten und/oder zweiten Teil des geheimen Schlüssels mit einem ein- oder mehrstufigen Algorithmus verknüpft werden, um einen Kanalkodierungsschlüssel zu erhalten. Vorzugsweise werden für die Bildung der Authentisierungsnachricht und des Kanalkodierungsschlüssels jeweils verschiedene Teile der vom Netzwerk erhaltenen Zufallszahl verwendet.

Eine weitere vorteilhafte Ausgestaltung der Erfindung sieht vor, daß der in der Karte abgelegte geheime Schlüssel sowie die Zufallszahl, welche vom Netzwerk an die Karte gesendet wird, in gleich lange Teile aufgeteilt werden. Damit kann in beiden Fällen der gleiche Berechnungsalgorithmus verwendet werden. Die Aufteilung der Zufallszahl bzw. des geheimen Schlüssels kann in der Weise erfolgen, daß eine einfache Teilung "in der Mitte" erfolgt oder sich überlappende Teilbereiche entstehen. Ebenso ist eine Teilung denkbar, in der die Summe der einzelnen Teile kleiner ist als die Bit-Länge der Zufallszahl bzw. des geheimen Schlüssels. Gemäß einer weiteren Variante können nach einem vorbestimmten Muster oder pseudozufällig jeweils eine vorgegebene Anzahl von Bits der Zufallszahl bzw. des geheimen Schlüssels zu jeweils einem Schlüssel- bzw. Zufallszahlenteil zusammengefaßt werden.

Als weitere vorteilhafte Ausgestaltung der Erfindung können als Berechnungsalgorithmen zur Authentisierung sowie zur Kanalkodierung DES-Algorithmen verwendet werden.

Eine andere vorteilhafte Variante der Erfindung sieht vor, daß zur Berechnung der Authentifizierungsparameter und der Kanalkodierungsschlüssel der vorzugsweise einstufige IDEA-Algorithmus verwendet wird.

Alternativ können zur Berechnung der Authentifizierungsparameter und der Kanalkodierungsschlüssel Komprimierungsalgorithmen, vorzugsweise kryptografische Komprimierungsalgorithmen verwendet werden, deren Ausgabewerte eine geringere Länge als die Eingabeparameter aufweisen.

Zur Erhöhung der Sicherheit ist es vorteilhaft, einen mindestens zweistufigen Berechnungsalgorithmus zu verwenden, wobei sich ein Triple-DES-Algorithmus als besonders sicher erweist. Bei diesem Algorithmus wird zunächst mit einem ersten Teil des Schlüssels und einem Teil der Zufallszahl verschlüsselt, anschließend wird eine Entschlüsselung des Ergebnisses mit dem zweiten Teil des Schlüssels vorgenommen, um schließlich wieder mit dem ersten Teil des Schlüssels eine weitere Berechnung auszuführen. Bei der letzten Verschlüsselung mit dem ersten Teil des Schlüssels kann in vorteilhafter Weise, insbesondere bei einer Schlüsselaufteilung in drei Schlüsselteile, ein neuer, dritter Schlüssel verwendet werden.

Eine weitere vorteilhafte Ausgestaltung der Erfindung ergibt sich, wenn die Auswahl des ersten oder zweiten Teils der Zufallszahl für die Authentisierung bzw. die Berechnung der Kanalkodierung im Wechsel erfolgt, wobei dieser Wechsel zufällig bzw. pseudozufällig ausgeführt wird und die Auswahl in der Karte und im Netzwerk auf die gleiche Weise erfolgt.

Im folgenden wird die Erfindung an Hand der Figuren 1 bis 3 näher beschrieben.

Fig. 1 zeigt den Ablauf der kryptographischen Funktionen des SIM im GSM-Netz.

Fig. 2 zeigt ein Blockschaltbild der Triple DES-Verschlüsselung.

Fig. 3 zeigt Beispiele für die Aufteilung des geheimen Schlüssels bzw. der Zufallszahl

Bei dem in Fig. 1 dargestellten Ablauf wird vorausgesetzt, daß der übliche, vorhergehende Vorgang der PIN-Verifizierung abgeschlossen ist. Im Anschluß daran wird von der mobilen Einheit, in der sich die Karte SIM befindet, eine Nachricht an das Netzwerk gesendet, welche eine IMSI- (international mobile subscriber identity) Information bzw. eine TMSI- (temporary mobile subscriber identity) Information enthält. Aus der IMSI bzw. TMSI wird im Netzwerk nach einer vorgegebenen Funktion oder mittels einer Tabelle ein geheimer Schlüssel K_i bestimmt. Derselbe Schlüssel ist auch in der Chipkarte SIM in einem nicht zugänglichen Speicherbereich abgelegt. Der geheime Schlüssel wird für die spätere Verifizierung des Authentisierungsvorganges benötigt.

Das Netzwerk initiiert sodann den Authentisierungsvorgang, indem es eine Zufallszahl RAND berechnet und diese über die Luftschnittstelle an die Chipkarte SIM überträgt.

In der Chipkarte wird daraufhin mittels eines Authentisierungsalgorithmus aus dem geheimen Schlüssel K_i und der Zufallszahl RAND ein Authentisierungsparameter SRES gebildet, der über die Luftschnittstelle wiederum an das Netzwerk übertragen wird. Erfindungsgemäß werden hierbei aus der

Zufallszahl RAND mindestens zwei Zufallszahlen $RAND_1$ und $RAND_2$ abgeleitet. Die Zufallszahlen $RAND_1$ und $RAND_2$ können durch Teilung oder eine Auswahl aus der Zufallszahl RAND bzw. durch einen Berechnungsalgorithmus gewonnen werden.

Die Authentisierung erfolgt im Ausführungsbeispiel nach Fig. 1 mit einem zweistufigen Algorithmus. Dabei wird, wie in Fig. 1 angedeutet, zunächst der erste Teil der Zufallszahl $RAND_1$ mit einem ersten Teil K_1 des ebenfalls in zwei Teile aufgeteilten Schlüssels K_i verschlüsselt. Das Ergebnis dieser ersten Stufe wird anschließend in einer zweiten Stufe mit dem zweiten Teil des Schlüssels K_2 verschlüsselt. Selbstverständlich kann zur Berechnung mit dem Authentisierungsalgorithmus zunächst auch der zweite Teil der Zufallszahl $RAND_2$ verwendet und die Reihenfolge der Verwendung der ersten und zweiten Schlüsselteile K_1 und K_2 verändert werden.

Im Netzwerk wird währenddessen auf dieselbe Weise wie in der Karte mittels des Authentisierungsalgorithmus und der Zufallszahl RAND ($RAND_1$, $RAND_2$) sowie dem geheimen Schlüssel K_i (K_1, K_2) ebenfalls ein Authentisierungsparameter SRES' gebildet. Der Parameter SRES' wird im Netzwerk sodann mit dem von der Karte erhaltenen Authentisierungsparameter SRES verglichen. Stimmen beide Authentisierungsparameter SRES' und SRES überein, wird der Authentisierungsvorgang erfolgreich abgeschlossen. Stimmen die Authentisierungsparameter nicht überein, gilt die Karte des Teilnehmers als nicht authentisiert. Es sei an dieser Stelle angemerkt, daß zur Bildung von SRES bzw. SRES' auch nur Teile aus dem durch die Verschlüsselung erhaltenen Ergebnisses verwendet werden können.

In der gleichen Weise wie die Erzeugung der Authentisierungsparameter erfolgt in der Karte und im Netzwerk die Generierung eines Schlüssels K_c

für Kanalkodierung für die Daten- und Sprachübertragung. Vorzugsweise wird dabei als Eingangsparameter der bei der Authentisierung nicht verwendete Teil der Zufallszahl RAND verwendet.

Figur 2 zeigt ein vorteilhaftes Ausführungsbeispiel, demgemäß die Berechnung mit dem Authentisierungsalgorithmus und/oder die Kanalcodierung durch einen Triple-DES-Algorithmus ausgeführt wird. Nach diesem Algorithmus wird zunächst ein Teil $RAND_1$ oder $RAND_2$ der Zufallszahl mit einem ersten Schlüsselteil K_1 verschlüsselt. Im nächsten Schritt erfolgt eine Entschlüsselung mit K_2. Das Ergebnis wird danach wieder mit K_1 oder bei einer Aufteilung in mehrere Zufallszahlen-/Schlüsselteile mit einem dritten Teil des Schlüssels verschlüsselt. Die Bildung der Kanalcodierung erfolgt auf die gleiche Weise. Im Netzwerk werden jeweils die entsprechenden Algorithmen verwendet.

Ohne Beschränkung der Allgemeinheit wurde bei der Beschreibung der Ausführungsbeispiele gemäß den Fig. 1 und 2 von einem zwei- bzw. dreistufigen, symmetrischen Verschlüsselungsalgorithmus ausgegangen. Selbstverständlich kann der Erfindungsgedanke, welcher in der Aufteilung der Zufallszahl sowie des geheimen Schlüssels besteht, auch mit anderen, gängigen Verschlüsselungs- bzw. Berechnungsalgorithmen durchgeführt werden. Beispielhaft sei hier neben den DES-Algorithmen (A3; A8) IDEA genannt. Die genannten Algorithmen können auch einstufig ausgeführt sein, wobei vorzugsweise unterschiedliche Teile des Schlüssels und/oder der Zufallszahl für die Authentisierung und die Erzeugung des Kanalkodierungsschlüssels K_c erzeugt werden.

In den Figuren 3a - e sind Beispiele für mögliche Aufteilungen des geheimen Schlüssels K_i bzw. der Zufallszahl RAND angegeben.

Die Figur 3a zeigt einen Schlüssel K_i bzw. eine Zufallszahl RAND mit einer Länge von 128 bit.

In der Figur 3b ist eine Aufteilung in zwei gleiche Teile K_1 und K_2 ($RAND_1$, $RAND_2$) dargestellt, wobei die Aufteilung mittig erfolgt. Teil 1 enthält bit 1 bis bit 64, Teil 2 enthält bit 65 bis bit 128. In Figur 3c ist eine überlappende Aufteilung angegeben und in der Figur 3d ist eine Aufteilung dargestellt, bei der jeweils die ungeradzahligen bits dem Teil 1 und die geradzahligen bits dem Teil 2 zugeordnet sind. Figur 3e zeigt schließlich eine Aufteilung, bei der die Summe der Binärstellen der Teile 1 und 2 kleiner ist als die Binärstellen des Ausgangsschlüssels bzw. der Ausgangszufallszahl.

Patentansprüche

1. Verfahren zur Authentisierung einer Chipkarte (SIM) in einem Netzwerk zur Nachrichtenübertragung, vorzugsweise in einem GSM-Netzwerk, bei dem in einer Chipkarte (SIM) ein Algorithmus sowie ein geheimer Schlüssel gespeichert sind, wobei zur Authentisierung
- zunächst vom Netzwerk oder einer Netzwerkkomponente eine Zufallszahl (RAND) an die Chipkarte übertragen wird,
- in der Chipkarte daraus mittels des Algorithmus und des geheimen Schlüssels (K_i)ein Antwortsignal (SRES) erzeugt und an das Netzwerk bzw. die Netzwerkkomponente übermittelt wird,
dadurch **gekennzeichnet**, daß
- zur Bildung eines Authentisierungsparameters der geheime Schlüssel (K_i) sowie die Zufallszahl (RAND) in jeweils wenigstens zwei Teile (K_1, K_2; $RAND_1$, $RAND_2$) aufgeteilt werden,
- einer der Teile ($RAND_1$, $RAND_2$) der übertragenen Zufallszahl (RAND) mit Hilfe eines oder mehrerer Teile (K_1, K_2) des geheimen Schlüssels (K_i) mittels eines ein- oder mehrstufigen, vorzugsweise symmetrischen Algorithmus verschlüsselt werden, und
- eine vorgegebene Anzahl von Bits aus dem Verschlüsselungsergebnis ausgewählt und als Signalantwort (SRES) an das Netzwerk übertragen wird.

2. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß der geheime Schlüssel (Ki) und/oder die Zufallszahl (RAND) in zwei Teile aufgeteilt werden.

3. Verfahren nach Anspruch 1 oder 2, dadurch **gekennzeichnet**, daß ein Teil der übertragenen Zufallszahl (RAND) sowie ein und/oder weite-

re Teile des geheimen Schlüssels (Ki) zur Berechnung eines Kanalkodierungsschlüssels (K_c) mittels eines ein- oder mehrstufigen Algorithmus verwendet werden, wobei zumindest ein Teil des Berechnungsergebnisses als Kanalkodierungsschlüssel (K_c) verwendet wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch **gekennzeichnet**, daß der Schlüssel (K_i) sowie die Zufallszahl (RAND) in zwei gleich lange Teile (K_1, K_2/$RAND_1$, $RAND_2$) aufgeteilt werden.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch **gekennzeichnet**, daß zur Berechnung der Authentifizierungsparameter (SRES, SRES´) und/oder des Kanalkodierungsschlüssels (K_c) DES-Algorithmen verwendet werden.

6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch **gekennzeichnet**, daß zur Berechnung der Authentisierungsparameter (SRES, SRES´) und/oder des Kanalkodierungsschlüssels (K_c) der, vorzugsweise einstufige, IDEA-Algorithmus verwendet wird.

7. Verfahren nach einem der Ansprüche 1 bis 4, dadurch **gekennzeichnet**, daß zur Berechnung der Authentisierungsparameter (SRES, SRES´) und/oder des Kanalkodierungsschlüssels (K_c) ein Komprimierungsalgorithmus verwendet wird, dessen Ausgabewert eine geringere Länge als der Eingabeparameter aufweist.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch **gekennzeichnet**, daß die Berechnung in einem mindestens zweistufigen Algorithmus erfolgt.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch **gekennzeichnet**, daß als Verschlüsselungsalgorithmus ein Triple-DES-Algorithmus verwendet wird, bei dem zunächst mit dem ersten Teil (K_1) des Schlüssels (K_i) verschlüsselt, anschließend mit dem zweiten Teil (K_2) des Schlüssels (K_i) entschlüsselt und darauf wieder mit dem ersten Teil (K_1) oder einem dritten Teil des Schlüssels (K_i) verschlüsselt wird.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch **gekennzeichnet**, daß eine Auswahl des ersten oder zweiten Teils der Zufallszahl (RAND) im zufälligen oder pseudozufälligen Wechsel in der Karte und im Netzwerk in gleicher Weise erfolgt.

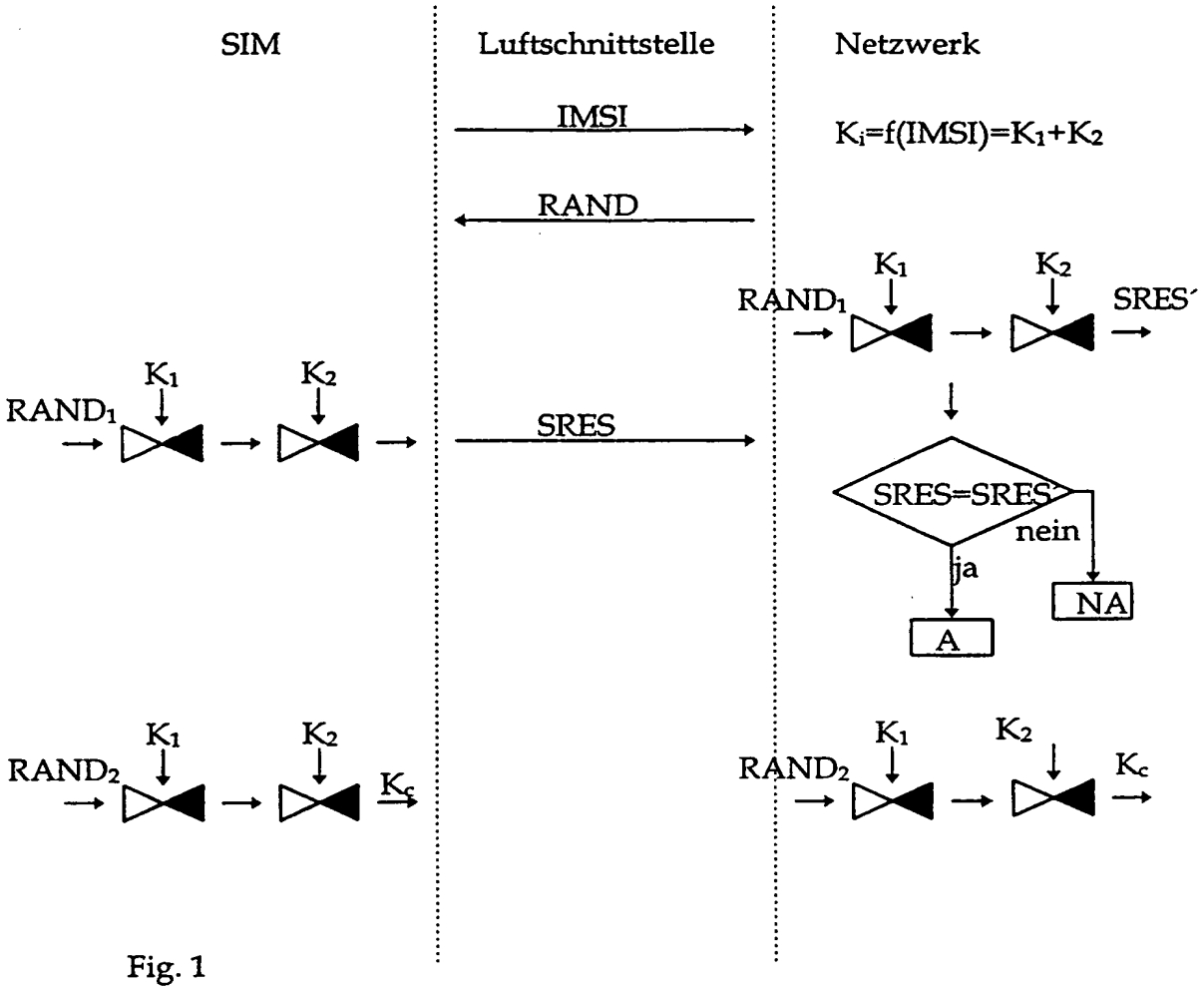

SIM
Luftschnittstelle
Netzwerk
IMSI
$K_i=f(IMSI)=K_1+K_2$
RAND
K_1
K_2
$RAND_1$
SRES´
SRES
SRES=SRES´
nein
ja
NA
A
$RAND_2$
K_c

Fig. 1

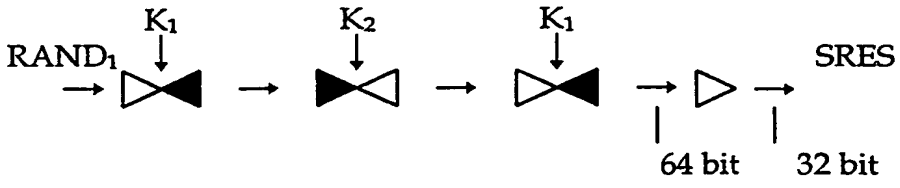

K_1
K_2
K_1
$RAND_1$
SRES
64 bit
32 bit

Fig. 2

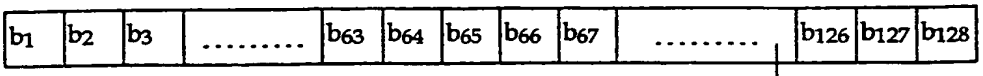


Fig. 3a

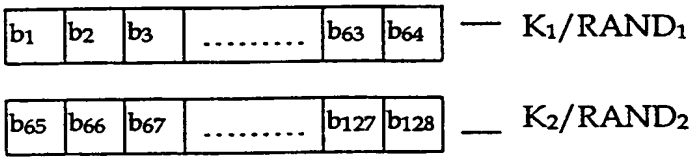


Fig. 3b

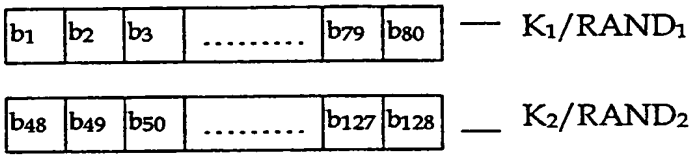


Fig. 3c

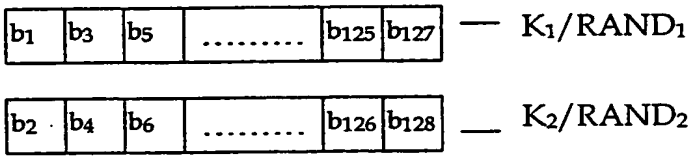


Fig. 3d

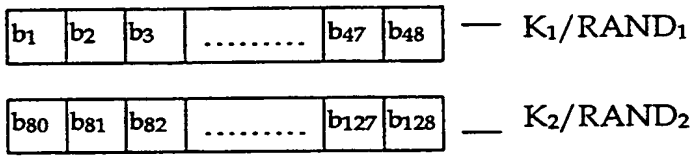


Fig. 3e

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 99/02848

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F G07C E05B H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and. where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 502 446 A (SIEMENS AG) 9 September 1992 (1992-09-09) the whole document ---	1,3
A	EP 0 840 480 A (MATSUSHITA ELECTRIC IND CO LTD ;TOKYO SHIBAURA ELECTRIC CO (JP)) 6 May 1998 (1998-05-06) abstract; figures 3,7 column 3, line 44 - column 5, line 38 column 7, line 49 - column 13, line 25 ---	1
A	EP 0 098 437 A (HUELSBECK & FUERST) 18 January 1984 (1984-01-18) abstract; figures page 9, line 15 - page 18, line 6 --- -/--	1

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 August 1999	31/08/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. ational Application No
PCT/EP 99/02848

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	DE 34 26 006 A (PHILIPS NV) 7 February 1985 (1985-02-07) abstract; figure 1 page 4, line 1 - page 9, line 30	1

1

INTERNATIONAL SEARCH REPORT

Int. ational Application No
PCT/EP 99/02848

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0502446 A	09-09-1992	AT 145511 T	15-12-1996
		DE 59207527 D	02-01-1997
		ES 2095339 T	16-02-1997
EP 0840480 A	06-05-1998	CN 1215271 A	28-04-1999
		JP 10233771 A	02-09-1998
EP 0098437 A	18-01-1984	DE 3225754 A	12-01-1984
		JP 1689338 C	11-08-1992
		JP 3058031 B	04-09-1991
		JP 59048567 A	19-03-1984
		US 4509093 A	02-04-1985
DE 3426006 A	07-02-1985	FR 2549989 A	01-02-1985
		GB 2144564 A,B	06-03-1985
		JP 1706001 C	27-10-1992
		JP 3074432 B	26-11-1991
		JP 60049471 A	18-03-1985
		SE 460157 B	11-09-1989
		SE 8403867 A	30-01-1985
		US 4612413 A	16-09-1986

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/02848

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G07F7/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G07F G07C E05B H04L H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 502 446 A (SIEMENS AG) 9. September 1992 (1992-09-09) das ganze Dokument ---	1,3
A	EP 0 840 480 A (MATSUSHITA ELECTRIC IND CO LTD ;TOKYO SHIBAURA ELECTRIC CO (JP)) 6. Mai 1998 (1998-05-06) Zusammenfassung; Abbildungen 3,7 Spalte 3, Zeile 44 - Spalte 5, Zeile 38 Spalte 7, Zeile 49 - Spalte 13, Zeile 25 ---	1
A	EP 0 098 437 A (HUELSBECK & FUERST) 18. Januar 1984 (1984-01-18) Zusammenfassung; Abbildungen Seite 9, Zeile 15 - Seite 18, Zeile 6 --- -/--	1

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
23. August 1999	31/08/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/02848

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 34 26 006 A (PHILIPS NV) 7. Februar 1985 (1985-02-07) Zusammenfassung; Abbildung 1 Seite 4, Zeile 1 - Seite 9, Zeile 30	1

1

INTERNATIONALER RECHERCHENBERICHT

Int. ...tionales Aktenzeichen
PCT/EP 99/02848

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0502446 A	09-09-1992	AT 145511 T	15-12-1996
		DE 59207527 D	02-01-1997
		ES 2095339 T	16-02-1997
EP 0840480 A	06-05-1998	CN 1215271 A	28-04-1999
		JP 10233771 A	02-09-1998
EP 0098437 A	18-01-1984	DE 3225754 A	12-01-1984
		JP 1689338 C	11-08-1992
		JP 3058031 B	04-09-1991
		JP 59048567 A	19-03-1984
		US 4509093 A	02-04-1985
DE 3426006 A	07-02-1985	FR 2549989 A	01-02-1985
		GB 2144564 A,B	06-03-1985
		JP 1706001 C	27-10-1992
		JP 3074432 B	26-11-1991
		JP 60049471 A	18-03-1985
		SE 460157 B	11-09-1989
		SE 8403867 A	30-01-1985
		US 4612413 A	16-09-1986